

**Cryptographic key generation system for private communication - generates public key from private-key information of terminal equipment NoAbstract**  
**Patent Assignee: MATSUSHITA ELEC IND CO LTD**

#### Patent Family

Patent Number	Kind	Date	Application Number	Kind	Date	Week	Type
JP 4245287	A	19920901	JP 9110630	A	19910131	199241	B
JP 3027988	B2	20000404	JP 9110630	A	19910131	200022	

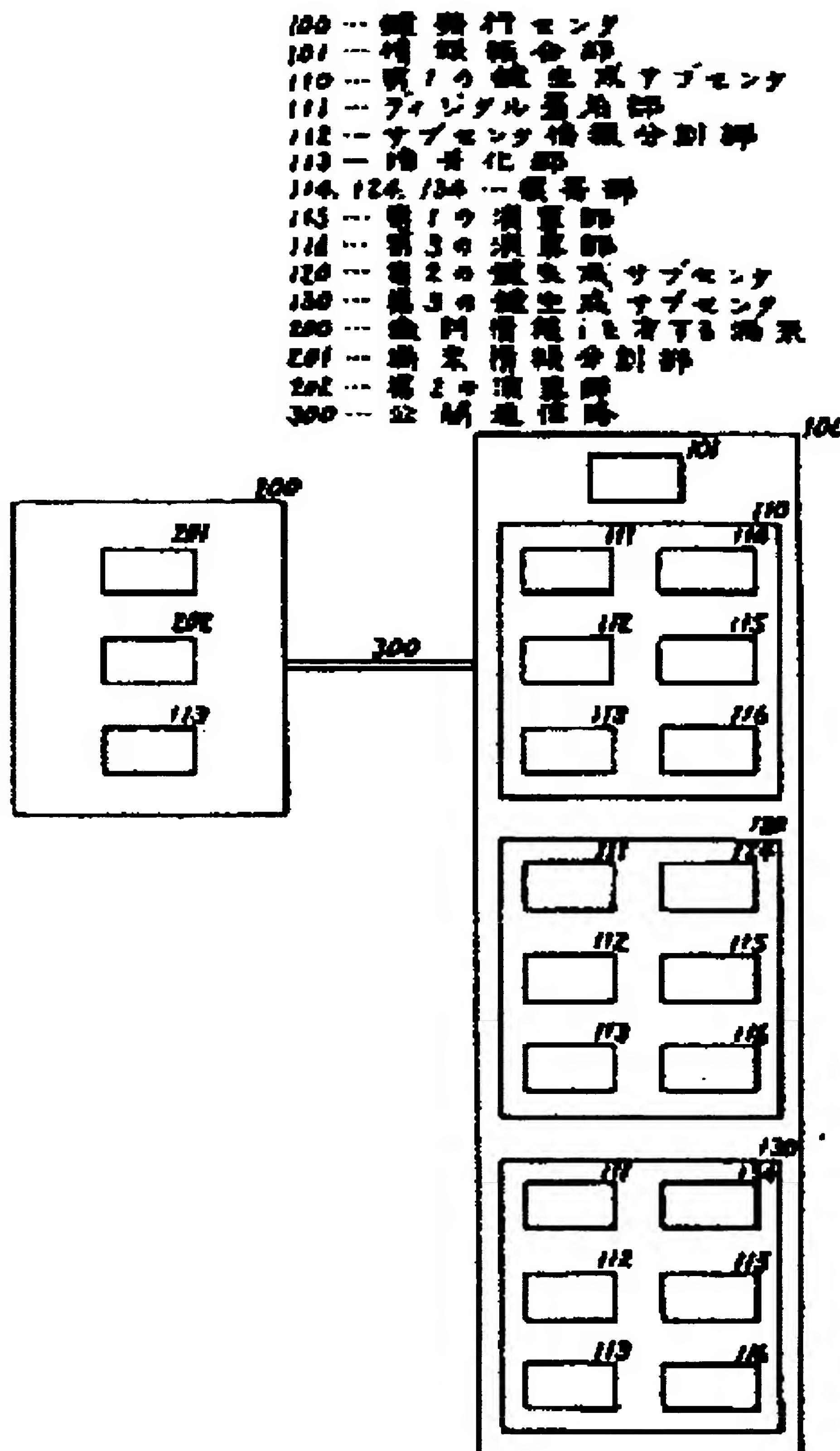
**Priority Applications (Number Kind Date): JP 9110630 A ( 19910131)**

#### Patent Details

Patent	Kind	Language	Page	Main IPC	Filing Notes
JP 4245287	A		6	G09C-001/00	
JP 3027988	B2		8	H04L-009/08	Previous Publ. patent JP 4245287

**BEST AVAILABLE COPY**

[図 1 ]



BEST AVAILABLE COPY

Derwent World Patents Index  
© 2005 Derwent Information Ltd. All rights reserved.  
Dialog® File Number 351 Accession Number 9210738

**BEST AVAILABLE COPY**

<http://toolkit.dialog.com/intranet/cgi/present?STYLE=621875714&PRESENT=DB=351,A...> 4/25/2006

(19)日本国特許庁 (JP)

## (12) 公開特許公報 (A)

(11)特許出願公開番号

特開平4-245287

(43)公開日 平成4年(1992)9月1日

(51) Int.Cl. <sup>5</sup>	識別記号	序内整理番号	F I	技術表示箇所
G 0 9 C	1/00	7922-5L		
H 0 4 L	9/28			
		7117-5K	H 0 4 L 9/02	A

審査請求 未請求 請求項の数 3 (全 6 頁)

(21)出願番号 特願平3-10630

(22)出願日 平成3年(1991)1月31日

(71)出願人 000005821  
 松下電器産業株式会社  
 大阪府門真市大字門真1006番地

(72)発明者 原田 俊治  
 大阪府門真市大字門真1006番地 松下電器  
 産業株式会社内

(72)発明者 松崎 なつめ  
 大阪府門真市大字門真1006番地 松下電器  
 産業株式会社内

(72)発明者 館林 誠  
 大阪府門真市大字門真1006番地 松下電器  
 産業株式会社内

(74)代理人 弁理士 小鍛治 明 (外2名)

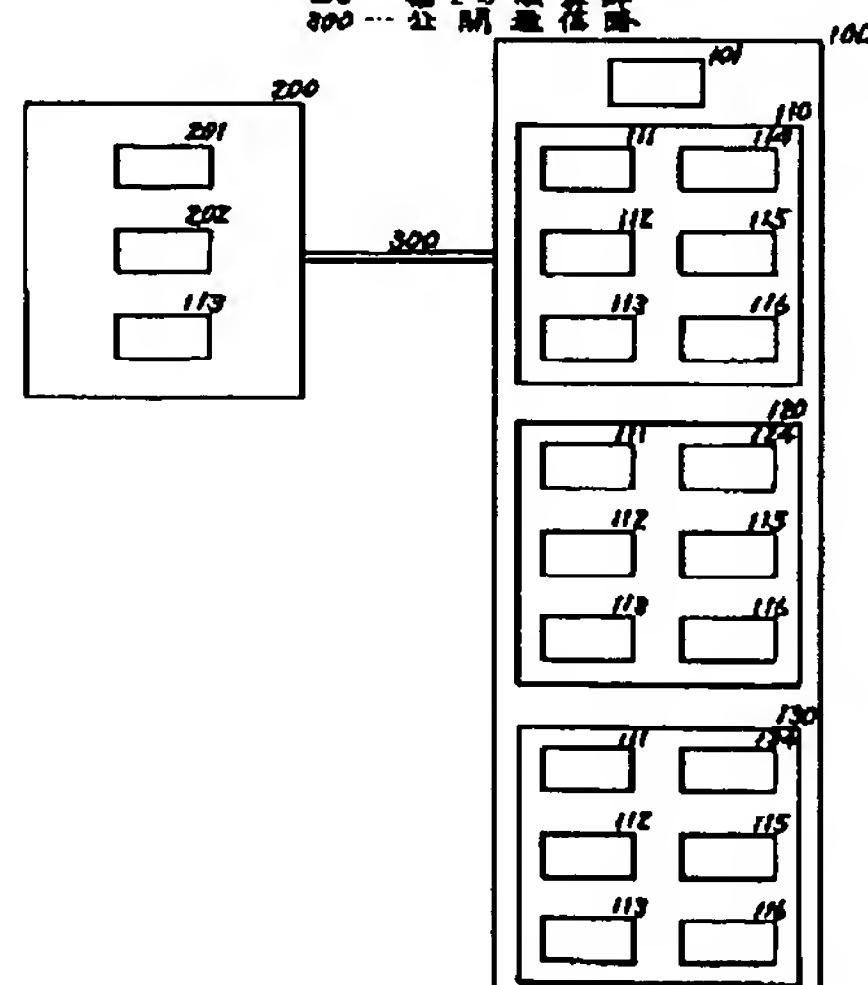
(54)【発明の名称】識別情報に基づく秘密鍵生成方式

## (57)【要約】

【構成】 端末の秘密鍵の部分情報を生成する複数の鍵生成サブセンタ110、120、130と、端末秘密情報を有する端末200が、以上情報をそれぞれを秘密に保ちつつ、端末秘密鍵情報を生成するために、鍵生成サブセンタにサブセンタ情報分割部112と暗号化部113と復号部114と第1の演算部115と第1の演算部116を設け端末に、端末情報分割部201と暗号化部113を設け、さらに端末に、その端末秘密鍵情報と端末秘密情報をから端末秘密鍵を生成するため第2の演算部202を設ける。

【効果】 端末の秘密鍵の部分情報を、端末の保持する端末秘密情報をから、端末の秘密鍵を、各鍵生成サブセンタや鍵発行センタに秘密に保ちつつ生成でき、鍵発行センタおよび鍵生成サブセンタに不正を防ぐことができる。

100-鍵発行センタ  
 101-情報鍵生成部  
 110-第1の鍵生成サブセンタ  
 111-ディジタル署名部  
 112-サブセンタ情報分割部  
 113-暗号化部  
 114-124-復号部  
 115-演算部  
 116-第2の演算部  
 120-第1の鍵生成サブセンタ  
 130-第3の鍵生成サブセンタ  
 200-端末  
 201-端末情報分割部  
 202-端末情報分割部  
 203-公開鍵情報



## 【特許請求の範囲】

【請求項 1】 鍵発行センタと端末とそれらを結ぶ公開通信路からなるシステムにおいて、前記鍵発行センタは、複数の鍵生成サブセンタと、複数の情報を一つの情報に結合する情報結合部を備え、前記各鍵生成サブセンタは、マスター公開鍵とそれぞれのサブセンタ秘密鍵を有し、さらに前記サブセンタ秘密鍵を用いてデジタル署名を生成するデジタル署名部と、一つの情報を複数の情報に分割するサブセンタ情報分割部と、前記各鍵生成サブセンタそれぞれに向けて情報の暗号化を行う暗号化部と、自身に向けられた暗号化された情報を復号する復号部と、第 1 の演算部を備え、前記端末は、マスター公開鍵と公開の端末識別情報と端末秘密情報を有し、さらに一つの情報を複数の情報に分割する端末情報分割部と、前記各鍵生成サブセンタそれぞれに向けて情報の暗号化を行う暗号化部と、第 2 の演算部を備え、前記端末が、前記端末秘密情報を、前記端末情報分割部に入力し、その出力として、複数の端末秘密部分情報を生成し、これらの端末秘密部分情報を、それぞれ前記暗号化部で暗号化し、その出力として暗号化された端末秘密部分情報を生成し、前記端末識別情報と、前記暗号化された端末秘密部分情報を、前記鍵発行センタに前記公開通信路を介して通知し、端末秘密鍵情報の発行を要求する端末秘密鍵情報要求ステップと、前記鍵発行センタが、前記各鍵生成サブセンタに、端末より通知された、前記端末識別情報と前記暗号化された端末秘密部分情報を通知し、端末秘密鍵部分情報の生成を依頼する端末秘密鍵部分情報生成依頼ステップと、前記各鍵生成サブセンタが、通知された前記端末識別情報を、前記デジタル署名部に入力し、その出力として端末部分秘密鍵を求め、この端末部分秘密鍵を、前記サブセンタ情報分割部に入力し、その出力として複数の端末部分秘密鍵部分情報を生成し、これらの端末部分秘密鍵部分情報を、それぞれ、前記暗号化部で暗号化し、その出力として暗号化された端末部分秘密鍵部分情報を生成し、これらの暗号化された端末部分秘密鍵部分情報を、それぞれ前記各鍵生成サブセンタに通知し、前記各鍵生成サブセンタが、それぞれ、前記各鍵生成サブセンタより通知された前記暗号化された端末秘密部分情報と前記鍵発行センタより通知された前記暗号化された端末秘密部分情報の中で、自信に向けられた情報を、前期復号部で復号し、その出力として、自信に向けられた前記端末部分秘密鍵部分情報と前記端末秘密部分情報を生成し、これらの端末部分秘密鍵部分情報と端末秘密部分情報を、前記第 1 の演算部に入力し、その出力として、端末秘密鍵部分情報を生成し、この端末秘密鍵部分情報を、前記鍵発行センタに通知する端末秘密鍵部分情報生成ステップと、前記鍵発行センタが、前記各鍵生成サブセンタからそれぞれ通知された前記端末秘密鍵部分情報を、前記情報結合部で結合し、その出力として、端末秘密鍵情報を生成し、こ

の端末秘密鍵情報を、公開通信路を介して、前記端末に通知する端末秘密鍵情報発行ステップと、前記端末が、通知された前期端末秘密鍵情報と前記端末秘密情報を、前記第 2 の演算部に入力し、その出力として、端末の秘密鍵を生成する端末秘密鍵生成ステップより構成される識別情報に基づく秘密鍵生成方式。

【請求項 2】 各鍵生成サブセンタは、請求項 1 の構成に加えて第 3 の演算部を備え、新たに、マスタ鍵生成ステップを追加し、そのマスタ鍵生成ステップにおいて、前記各鍵生成サブセンタの有するサブセンタ秘密鍵を、前期サブセンタ情報分割部に入力し、その出力として、複数のサブセンタ秘密鍵部分情報を生成し、このサブセンタ秘密鍵部分情報を、それぞれ、前記暗号化部で暗号化し、その出力として、暗号化されたサブセンタ秘密鍵部分情報を生成し、これらの暗号化されたサブセンタ秘密鍵部分情報を、前記各鍵生成サブセンタに通知し、前記各鍵生成サブセンタが、前記各鍵生成サブセンタより通知された前記暗号化されたサブセンタ秘密鍵部分情報の中で、自信に向けられた情報を、前記復号部で復号し、20 その出力として、自信に向けられた前記サブセンタ秘密鍵部分情報を生成し、これらのサブセンタ秘密鍵部分情報を第 3 の演算部に入力し、その出力としてマスタ公開鍵部分情報を求め、そのマスタ公開鍵部分情報を鍵発行センタに通知し、前記鍵発行センタは、通知された前記マスタ公開鍵部分情報を、前記情報結合部に入力し、その結果をマスタ鍵とすることを特徴とする特許請求の範囲第 1 項記載の秘密鍵生成方式。

【請求項 3】 マスタ鍵生成ステップにおいて、第 1 のマスタ公開鍵  $e$  と、第 1 のサブセンタ秘密鍵として素数  $p_j$  と、第 2 のサブセンタ秘密鍵として、 $(p_j-1)$  を法とする前記  $e$  の乗法的逆数  $d_j$  を有する鍵生成サブセンタ  $j$  ( $1 \leq j \leq n$ ) が、前記第 1 のサブセンタ秘密鍵  $p_j$  を前期サブセンタ情報分割部に入力し、その出力として、複数のサブセンタ秘密鍵部分情報  $p_{jk}$  ( $1 \leq k \leq n$ ) を生成し、これらの  $p_{jk}$  を、それぞれ、前期暗号化部  $E_k$  ( $1 \leq k \leq n$ ) で、暗号化し、その出力として暗号化されたサブセンタ秘密鍵部分情報  $E_k(p_{jk})$  ( $1 \leq k \leq n$ ) を生成し、これらの  $E_k(p_{jk})$  を、それぞれ前期各鍵生成サブセンタに通知し、鍵生成サブセンタ  $k$  ( $1 \leq k \leq n$ ) が、前記各鍵生成サブセンタより通知された前記  $E_k(p_{jk})$  ( $1 \leq j \leq n$ ) を、それぞれ、前期復号部で復号し、前記サブセンタ秘密鍵部分情報  $p_{jk}$  ( $1 \leq j \leq n$ ) を求め、この  $p_{jk}$  ( $1 \leq j \leq n$ ) を、第 3 の演算部に入力し、前記  $p_{jk}$  ( $1 \leq j \leq n$ ) の積  $P_k$  を求め、この  $P_k$  をマスタ公開鍵部分情報として前記鍵発行センタに通知し、前記鍵発行センタは、通知された前記マスタ公開鍵部分情報  $P_k$  ( $1 \leq k \leq n$ ) を、前記情報結合部に入力し、その出力として第 2 のマスタ公開鍵  $P$  を生成し、前期端末秘密鍵情報要求ステップで、端末秘密情報  $r$  と、識別情報  $i$  を有する端末が、前記  $r$  を前期端末情報分割部に入力し、その出力

として端末秘密部分情報rk ( $1 \leq k \leq n$ ) を生成し、このrkを、それぞれ、前期暗号化部Ek ( $1 \leq k \leq n$ ) で暗号化し、その出力として、暗号化された端末秘密部分情報Ek (rk) を生成し、前記端末識別情報1と前記Ek(rk) ( $1 \leq k \leq n$ ) を前記鍵発行センタに通知し、端末秘密鍵部分情報生成依頼ステップで、前記鍵発行センタが、前記各鍵生成サブセンタj ( $1 \leq j \leq n$ ) に、前記端末識別情報1と、前記暗号化された端末秘密部分情報Ej(rj) ( $1 \leq j \leq n$ ) を通知し、端末秘密鍵部分情報生成ステップで、鍵生成サブセンタj ( $1 \leq j \leq n$ ) は、前記端末識別情報1を、デジタル署名部に入力し、その出力として、次式を満たすSJ

$$Sj = aj \times bj \times (i^{d1} \bmod p_j)$$

ただし  $aj = P/p_j$

$$bj \times aj = 1 \bmod p_j$$

を端末部分秘密鍵として求め、このSJを、前記サブセンタ情報分割部に入力し、複数の端末部分秘密鍵部分情報Sjk ( $1 \leq k \leq n$ ) を生成し、このSjkを、前期暗号化部Ek ( $1 \leq k \leq n$ ) で、暗号化し、その出力として、前記暗号化された端末部分秘密鍵部分情報Ek(Sjk) ( $1 \leq k \leq n$ ) を生成し、このEk(Sjk)を、前記各鍵生成サブセンタに通知し、鍵生成サブセンタk ( $1 \leq k \leq n$ ) が、前記各鍵生成サブセンタより通知された前記暗号化された端末部分秘密鍵部分情報Ek(Sjk) ( $1 \leq j \leq n$ ) と前記鍵発行センタから通知された前記暗号化された端末秘密部分情報Ek(rk)を、それぞれ前記復号部で復号し、前記端末部分秘密鍵部分情報Sjk ( $1 \leq j \leq n$ ) と前記端末秘密部分情報rkを求める、このSjk ( $1 \leq j \leq n$ ) と前記rkを、第1の演算部に入力し、前記Sjk ( $1 \leq j \leq n$ ) とrkそれぞれの和Sk'を、端末秘密鍵部分情報として求め、前記Sk'を、前記鍵発行センタに通知し、端末秘密鍵情報発行ステップで、前記鍵発行センタが、前記各鍵生成サブセンタから通知された前記端末秘密鍵部分情報Sk' ( $1 \leq k \leq n$ ) を、前記情報結合部で結合して端末秘密鍵情報Sを生成し、このSを前記公開通信路を用いて前記端末に通知し、端末秘密鍵生成ステップで、前記端末が、通知された前期端末秘密鍵情報Sと前記端末秘密情報rを、前記第2の演算部に入力して、前記Sとrの差Sを端末の秘密鍵を生成することを特徴とする特許請求の範囲第2項記載の秘密鍵生成方式。

【発明の詳細な説明】

【0001】

【産業上の利用分野】 本発明は、識別情報に基づく暗号方式における秘密鍵の生成方式に関する。

【0002】

【従来の技術】 識別情報に基づく暗号方式として、シャミアーナの提案したデジタル署名方式、太田の提案した認証方式、岡本および田中の提案した暗号鍵配達方式がある。(シャミアーナの方式は、"アイデンティティペースト クリプトシステム アンド シグネチャー ス 50

キームズ" プロシーディング オヴ クリプト 84 pp 47-53 1984.8に、太田の方式は、"RSA暗号系を利用した個人識別情報に基づく認証方式" 電子情報通信学会論文誌D-1 vol.72-D-1 N0.8 pp612-632 1989.8に、岡本及び田中の方式は、"ID情報に基づく暗号鍵配達方式の提案" 電子情報通信学会論文誌D-1 vol.72-D-1 N0.4 pp293-300 1989.4にそれぞれ詳しい。) これらの方は、いずれも、信頼のにおける単一の鍵発行センタが、各端末に対して、その端末固有の識別情報に対応する秘密鍵を発行する端末秘密鍵発行ステップと、各端末が、発行された秘密鍵を用いて、デジタル署名、相手認証、あるいは、鍵共有などの暗号プロトコルを実行する暗号プロトコル実行ステップからなる。これらの方はにおける端末秘密鍵発行ステップは、いずれも、RSAデジタル署名法を用いて次のように実行される。(RSAデジタル署名については、"現代暗号理論" 小山他著、電子情報通信学会編に詳しい。)

端末の秘密鍵発行ステップ

(1) 鍵発行センタの初期設定

鍵発行センタは、2素数p1, p2を生成し、それらの積Pを求め、 $L = \text{LCM}(p1-1, p2-1)$  に互いの素な数eを生成し、Lを法とする剰余環のなかで乗法的逆数dを生成し、Pは、端末に公開し、(p1, p2, d)は秘密に保持する。

(2) 端末による秘密鍵発行要求

端末は、固有の識別情報1を、鍵発行センタに通知し、秘密鍵の発行を要求する。

(3) 端末の秘密鍵生成

鍵発行センタは、端末の秘密鍵Siを、秘密鍵(p1, p2, d)を用いたRSAデジタル署名

$$Si = i^d \bmod P \quad (\text{ただし } P = p1 \times p2)$$

より求め、端末1に秘密に送る。ここで、 $(a \bmod b)$ は、aをbで割ったときの剰余を表わす。このようにして生成された秘密鍵Siを用いて、この後、各種暗号プロトコルが実行される。このような手順で端末の秘密鍵を発行する場合、鍵発行センタは任意の端末の秘密鍵を知ることができることは明かである。従って、仮にセンタが悪意を持ったとき、端末1の秘密鍵Siを鍵発行センタが悪用するすることが容易である。

【0003】

【発明が解決しようとする課題】 このように、従来の方では、単一の鍵発行センタが、デジタル署名によって端末の秘密鍵を生成するため、その鍵発行センタは、端末の秘密鍵を容易に知ることができ、鍵発行センタによって端末の秘密鍵を悪用されかねないという問題点を有している。本発明は、上述の問題点に鑑みて試されたもので、鍵発行センタが、端末の秘密鍵を知ることのできない、識別情報に基づく秘密鍵生成法を提供することを目的とする。

【0004】

【課題を解決するための手段】本発明は上述の問題点を解決するため、複数の鍵生成サブセンタと情報結合部からなる鍵発行センタと、サブセンタ秘密鍵を有し、さらに、サブセンタ秘密鍵を用いるディジタル署名部とサブセンタ情報分割部と暗号化部と復号部と第1の演算部と第3の演算部からなる鍵生成サブセンタと、端末秘密情報を有し、さらに、端末情報分割部と暗号化部と第2の演算部からなる端末と公開通信路からなるという構成を備えたものである。

【0005】

【作用】本発明は上述の構成によって、端末が、端末秘密情報を端末情報分割部で分割し、その結果を端末秘密部分情報として、各鍵生成サブセンタに秘密に通知し、鍵生成サブセンタが、端末の識別情報に対応する端末部分秘密鍵を、サブセンタ情報分割部で分割し、その結果を端末部分秘密鍵部分情報として、各鍵生成サブセンタに秘密に通知し、さらに各鍵サブセンタが、各鍵生成サブセンタから通知された端末部分秘密鍵部分情報と、端末より秘密に通知された端末秘密部分情報を第1の演算部に入力し、その出力として、端末秘密鍵部分情報を生成し、それを鍵発行センタに通知し、鍵発行センタが、その端末秘密鍵部分情報を、情報結合部で結合し、その結果として端末秘密鍵情報を生成し、それを、端末に通知し、端末が、その端末秘密鍵情報と端末秘密情報をから端末の秘密鍵を生成するため、鍵発行センタおよび鍵生成サブセンタに端末の秘密鍵が知られることがなく、鍵発行センタおよび鍵生成サブセンタのセンタの不正を防ぐことができる。

【0006】また、上述の構成によって、鍵生成サブセンタが、サブセンタ秘密鍵を、サブセンタ情報分割部で分割し、その結果としてサブセンタ秘密鍵部分情報を生成し、それを各鍵生成サブセンタに秘密に通知し、各鍵生成サブセンタが、通知されたサブセンタ秘密鍵部分情報を、第3の演算部に入力し、その出力としてマスタ公開鍵部分情報を生成し、それを鍵発行センタに通知し、鍵発行センタが、マスタ公開鍵部分情報を情報結合部で結合し、その結果として、マスタ公開鍵生成することができるため、サブセンタのサブセンタ秘密鍵を、秘密に保ちつつマスタ公開鍵を生成でき、鍵発行センタおよび鍵生成サブセンタのセンタの不正を防ぐことができる。

【0007】

【実施例】図1は本発明の一実施例による識別情報に基づく秘密鍵生成方式の概略構成を示すものであって、100は、端末に、端末秘密鍵情報を発行する鍵発行センタであり、200は、識別情報1を有する端末であり、300は、公開通信路であり100を構成する110、120、130は、それぞれ端末秘密鍵部分情報を生成する、第1の鍵生成サブセンタ、第2の鍵生成サブセンタ、第3の鍵生成サブセンタであり、101は、情報結合部であり、110を構成する111は、端末の部分秘

密鍵を生成するディジタル署名部であり、112は、サブセンタ情報分割部であり、113は、第1、第2、第3の暗号化関数からなる暗号化部であり、114は、第1の復号関数からなる復号部であり、115は、加算演算を行なう1の演算部であり、116は、乗算演算を行なう第3の演算部であり、120を構成する111は、端末の部分秘密鍵を生成するディジタル署名部であり、112は、サブセンタ情報分割部であり、113は、第1、第2、第3の暗号化関数からなる暗号化部であり、124は、第2の復号関数からなる復号部であり、115は、加算演算を行なう1の演算部であり、116は、乗算演算を行なう第3の演算部であり、130を構成する111は、端末の部分秘密鍵を生成するディジタル署名部であり、112は、サブセンタ情報分割部であり、113は、第1、第2、第3の暗号化関数からなる暗号化部であり、124は、第2の復号関数からなる復号部であり、115は、加算演算を行なう1の演算部であり、116は、乗算演算を行なう第3の演算部であり、200を構成する201は、端末秘密情報を分割する端末情報分割部であり、202は、減算演算を行なう第2の演算部であり、113は、第1、第2、第3の暗号化関数からなる暗号化部である。

【0008】次に、実施例の動作について述べる。

(1) マスタ公開鍵生成ステップ

第1の鍵生成サブセンタ110を例に述べる、第2、第3の鍵生成サブセンタ120、130も同様に動作する。

【0009】(1.1)サブセンタ秘密鍵部分情報の生成

第1の鍵生成サブセンタ110は、第1のマスタ公開鍵として素数eと、第1のサブセンタ秘密鍵として素数p1と、第2のサブセンタ秘密鍵として次式を満たすd1:  

$$e \times d1 = 1 \pmod{(p1 - 1)}$$

を保持し、このp1を、サブセンタ分割部112に入力し、p1の部分情報p1k (k=1, 2, 3)を生成する。なお、サブセンタ分割部112は、ある3個の数のそれぞれの分割値毎の積が、元の3個の数の積の分割値となる分割関数を有する。

【0010】(1.2)サブセンタ秘密鍵部分情報の暗号化と通知

40 第1の鍵生成サブセンタ110は、p1の部分情報p1k (k=1, 2, 3)を、暗号化部113で暗号化してE1(p1k) (k=1, 2, 3)を求め、E1(p11)は、保持し、E2(p12)、E3(p13)は、それぞれ、第2、第3の鍵生成サブセンタに通知する。

【0011】(1.3)サブセンタ秘密鍵部分情報の復号とマスタ公開鍵部分情報の生成

第1の鍵生成サブセンタ110は、通知されたE1(p11)、E1(p21)、E1(p31)を、復号部114で復号し、サブセンタ秘密鍵部分情報p11、p21、p31を求め、これらを50 第3の演算部116で、

$P1' = p1 \times p2 \times p3$

を求め、マスタ公開鍵部分情報として、鍵発行センタに通知する。なお、ここでの乗算は、ある有限環上での乗算である。

【0012】(1.4)マスタ公開鍵の生成

鍵発行センタは、通知された $P1'$ 、 $P2'$ 、 $P3'$ を情報結合部に入力し

$$P = P1' \times P2' \times P3' (= p1 \times p2 \times p3)$$

を求める。なお、ここでの乗算は、ある有限環上での乗算である。なお、情報結合部は、サブセンタ分割部の分割閾数の逆閾数を有する。

【0013】以上のステップにより、サブセンタ秘密鍵 $p1$ 、 $p2$ 、 $p3$ を秘密に保ちつつ、その積を求めることが可能である。

(2) 端末秘密鍵情報要求ステップ

(2.1) 端末秘密部分情報の生成

識別情報 $i$ を有する端末200は、端末秘密情報としてある乱数値 $r$ を保持し、この $r$ を、端末分割部201に入力し、端末秘密部分情報 $r_k$  ( $k=1, 2, 3$ )を生成する。なお、端末分割部201は、ある3個の数のそれぞれの分割値毎の和が、元の3個の数の和の分割値となる閾数を有する。

【0014】(2.2) 端末秘密部分情報の暗号化と端末秘密鍵情報の要求

端末200は、端末秘密部分情報 $r_k$  ( $k=1, 2, 3$ )を、暗号化部113で暗号化し、 $E_k(r_k)$  ( $k=1, 2, 3$ )を求める、識別情報 $i$ および $E1(r_1)$ 、 $E2(r_2)$ 、 $E3(r_3)$ を、それぞれ鍵発行センタに通知する。

(3) 端末秘密鍵部分情報生成依頼ステップ

端末から通知された識別情報 $i$ および $E1(r_1)$ 、 $E2(r_2)$ 、 $E3(r_3)$ を、それぞれ鍵生成サブセンタに通知する。

(4) 端末秘密鍵部分情報生成ステップ

第1の鍵生成サブセンタ110を例に述べる、第2、第3の鍵生成サブセンタ120、130も同様に動作する。

【0015】(4.1) 端末部分秘密鍵の生成

第1の鍵生成サブセンタは、前記端末識別情報 $i$ を、デジタル署名部111に入力し、端末部分秘密鍵 $S1$

$$S1 = a1 \times b1 \times (i^{d1} \bmod p1)$$

ただし  $a1 = P / p1 = p1 \times p2$

$$b1 \times a1 = 1 \bmod p1$$

を生成する。なお、ここでの乗算は、ある有限環上での乗算である。

【0016】(4.2) 端末部分秘密鍵部分情報の生成

端末部分秘密鍵 $S1$ を、サブセンタ情報分割部112に入力し、端末部分秘密鍵部分情報 $S11$ 、 $S12$ 、 $S13$ を生成する。なお、サブセンタ分割部201は、ある3個の数のそれぞれの分割値毎の和が、元の3個の数の和の分割値となる閾数を有する。

【0017】(4.2) 端末部分秘密鍵部分情報の暗号化と通知

端末部分秘密鍵部分情報 $S11$ 、 $S12$ 、 $S13$ を、暗号化部113で、暗号化し、 $E1(S11)$ 、 $E2(S12)$ 、 $E3(S13)$ を生成し $E1(S11)$ 、 $E2(S12)$ 、 $E3(S13)$ を、各鍵生成サブセンタに通知する。

【0018】(4.3) 端末部分秘密鍵部分情報の復号

各鍵生成サブセンタより通知された暗号化された端末部分秘密鍵部分情報 $E1(S11)$ 、 $E1(S21)$ 、 $E1(S31)$ と、前記鍵発行センタから通知された暗号化された端末秘密部分情報 $E1(r1)$ を、それぞれ復号部114で復号し、端末部分秘密鍵部分情報 $S11$ 、 $S21$ 、 $S31$ と、端末秘密部分情報 $r1$ を生成する。

【0019】(4.4) 端末秘密鍵部分情報の生成

端末部分秘密鍵部分情報 $S11$ 、 $S21$ 、 $S31$ と、端末秘密部分情報 $r1$ を第1の演算部115に入力して、その出力として、端末秘密鍵部分情報 $S1S1 = S11 + S21 + S31 + r1$ を生成し、鍵発行センタに通知する。なお、ここでの加算は、ある有限環上での加算である。

20 (5) 端末秘密鍵情報発行ステップ

鍵発行センタが、各鍵生成サブセンタから通知された端末秘密鍵部分情報 $S1'$ 、 $S2$ 、 $S3$ を、情報結合部101で結合して、端末秘密鍵情報 $S$ を生成し、この $S$ を公開通信路300を介して、端末200に発行する。なお、情報結合部は、サブセンタ分割部および端末の分割部の分割閾数の逆閾数を有する。

(6) 端末秘密鍵生成ステップ

端末が、通知された端末秘密鍵情報 $S$ と端末秘密情報 $r$ を、第2の演算部202に入力し、その出力として、端末の秘密鍵 $S$

$$S = S - r$$

を生成する。なお、ここでの減算は、ある有限環上での減算である。以上のステップにより、鍵生成サブセンタの生成した端末の部分秘密鍵 $S1$ 、 $S2$ 、 $S3$ 、および、端末秘密情報 $r$ を秘密に保ちつつ、秘密鍵 $S$ を求めることが可能である。

40 【0020】すなわち各鍵生成サブセンタは、生成した端末部分秘密鍵を、端末や他の鍵生成サブセンタや鍵発行センタに秘密に保ちつつ、また、端末は、端末の端末秘密情報を、各鍵生成サブセンタや鍵発行センタに秘密に保ちつつ、端末部分秘密鍵と端末秘密情報から端末秘密鍵情報が生成され、端末によって、その端末秘密鍵情報と端末秘密情報より端末の秘密鍵を生成できるため、鍵発行センタおよび鍵生成サブセンタに端末の秘密鍵が知られることなく、鍵発行センタの不正を防ぐことができる。

【0021】

【発明の効果】以上の説明から明らかなように、本発明は、鍵発行センタが端末の部分秘密鍵を生成する鍵生成50 サブセンタを複数備え、各鍵生成サブセンタが、端末よ

り秘密に通知された端末秘密部分情報と、各鍵生成サブセンタより秘密に通知された端末部分秘密鍵部分情報を、第1の演算部に入力して端末秘密鍵部分情報を求め、鍵発行センタが、情報結合部でその端末秘密鍵部分情報を結合して端末秘密鍵情報を生成し、端末が、その端末秘密鍵情報と端末秘密情報から端末秘密鍵を生成するという構成を備えることにより、各鍵生成センタ秘密情報である端末部分秘密鍵と端末の秘密情報である端末秘密情報を、秘密に保ちつつ、端末によって、端末の秘密鍵が生成できるため、鍵発行センタおよび鍵生成サブセンタに端末の秘密鍵が知られることがなく、鍵発行センタの不正を防ぐことができる。

【図面の簡単な説明】

【図1】本発明の実施例の構成図である。

【符号の説明】

100 鍵発行センタ

200	識別情報1を有する端末
300	公開通信路
101	情報結合部
110	第1の鍵生成サブセンタ
111	デジタル署名部
112	サブセンタ情報分割部
113	暗号化部
114	復号部
115	第1の演算部
10	116 第3の演算部
120	第2の鍵生成サブセンタ
124	復号部
130	第3の鍵生成サブセンタ
134	復号部
201	端末情報分割部
202	第2の演算部

【図1】

